

# PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-207197

(43)Date of publication of application : 28.07.2000

(51)Int.Cl.

G06F 9/06

(21)Application number : 11-007269

(71)Applicant : NEC CORP

(22)Date of filing : 14.01.1999

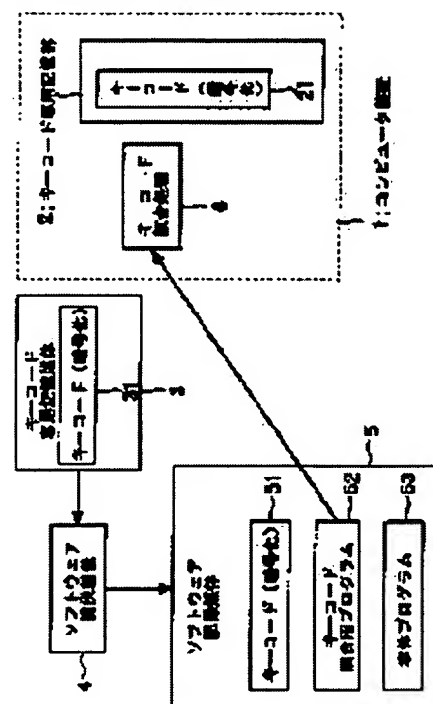
(72)Inventor : MURAMATSU KAZUE

## (54) SYSTEM AND METHOD FOR PROTECTING COMPUTER SOFTWARE

### (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent software from unauthorized use by collating identification information sent back from a software provider against the identification information of a computer.

**SOLUTION:** When providing a user with software, the software provider requests the user to input a key code and a software providing device 4 enciphers and records it on a recording medium of a software 5. On a software recording medium 5, the enciphered key code 51 and a program 52 for collating and deciding the key codes of the recording medium side and the computer main body side are recorded along with the provided (distributed) software 53. On the user's side, the computer 1 performs the collation and decision at the start of the use of the software and the use of the main body program 53 stored on the software recording medium 5 is made unauthorized, when the key code 51 on the side of the software recording medium 5 does not match the key code 21 of the computer main body 1.



\* NOTICES \*

JP0 and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

CLAIMS

---

[Claim(s)]

[Claim 1]In providing a user with software from a software provider, Receive identification information which is the peculiar identification information which a computer which said user uses holds, and was enciphered from said user, and in the software provider side. After checking decryption and validity of said identification information, with software distributed to said user. Said user is provided with a collation judgment program which performs collation processing of said identification information in the state where it enciphered, and said identification information and identification information of said user's computer, When said user uses said provided software by said user's computer, said collate program is executed on said computer, A protection method of computer software which compares whether identification information returned by software provider and identification information of said computer are mutually in agreement, and makes improper use of a program in said computer, and installation in not being in agreement.

[Claim 2]Encipher a peculiar key code currently assigned for every computer, carry out hold stores to a storage parts store only for a key code of said computer, and a software provider, A user who demands a key code currently assigned in software to a computer which uses this software at the time of offer, and uses software by said computer, Supply a recording medium holding an encryption key code of a computer body, and a key code of an identical content to said software provider, and the software provider side device, After canceling encryption of a key code supplied from said computer and checking compatibility, Said key code which enciphered software with which said computer is provided, Supply a recording medium stored with a collate program which cancels said code and compares a key code to said computer, and in said computer. A user executes said collate program stored in said recording medium at the time of use of software recorded on said recording medium, or installation, It is compared whether a code of a key code stored in said recording medium and a key code memorized by

storage parts store only for said key code of said computer is canceled, and these are in agreement, A protection method of computer software which makes improper use of a program in said computer, and installation in not being in agreement.

[Claim 3]Encipher a peculiar key code currently assigned for every computer, carry out hold stores to a storage parts store only for a key code of said computer, and a software provider, A user who demands a key code currently assigned in software to a computer which uses this software at the time of offer, and uses software by said computer, Supply an encryption key code of a computer body, and a key code of an identical content to said software provider via a communication line, and in said software provider side device. After canceling encryption of a key code supplied via said communication line of said computer and checking compatibility, Said key code which enciphered software with which said computer is provided, Via said communication line, supply said computer with a collate program which cancels a code and compares a key code, and in said computer. Software which was supplied via said communication line and with which said computer is provided, Once memorize to said enciphered key code, and a collate program and memory storage which cancel a code and compare a key code, and said collate program stored in said memory storage is executed at the time of use of said software, or installation, It is compared whether a code of a key code stored in said memory storage and a key code memorized by storage parts store only for a key code of said computer is canceled, and these are in agreement, A protection method of computer software which makes improper use of a program in said computer, and installation in not being in agreement.

[Claim 4]Equip 1 or two or more computers, and this computer with a software providing device which provides software, and said each computer, Where a peculiar key code currently assigned for every computer is enciphered, have a storage parts store only for a key code which carries out hold stores, and a software provider, A user who demands a key code currently assigned in software to a computer which uses this software at the time of offer, and uses software by said computer, To said software providing device, supply an encryption key code of said computer body, and a key code of an identical content with a recording medium to hold, and to it said software providing device, Where a means to cancel encryption of a key code supplied from said computer, a means to check the compatibility of a key code of which a code was canceled, and a key code by which compatibility was checked are enciphered, Software with which said computer is provided, and a means written in a software recording medium stored with a collate program which cancels said code and compares a key code, Said computer which supplied a preparation and said software recording medium to said computer, and received said software recording medium, At the time of use of software recorded on said software recording medium, or installation, said collate program stored in said software recording medium is executed, It has a means to compare whether a code of a

key code stored in said recording medium and a key code memorized by storage parts store only, for a key code of said computer is canceled, and these are in agreement, A protection system of computer software which makes improper use of a program in said computer, and installation when these key codes are not in agreement.

[Claim 5] 1 or two or more computers, and a software providing device that is connected to said computer via a communication line, and provides said computer with software, Where a peculiar key code currently assigned for every computer is enciphered, a preparation and said computer are provided with a storage parts store only for a key code which carries out hold stores, and a software provider, A user who demands a key code currently assigned in software to a computer which uses this software at the time of offer, and uses software by said computer, An encryption key code of said computer body and a key code of an identical content are transmitted to said software providing device via said communication line at said software providing device, A means for said software providing device to receive a key code transmitted via said communication line from said computer, and to cancel encryption of this key code, Where a means to check the compatibility of a key code of which a code was canceled, and a key code by which compatibility was checked are enciphered, It has software with which said computer is provided, and a means to transmit to said computer via said communication line with a collate program which cancels said code and compares a key code. Said computer was transmitted via said communication line from said software providing device. An enciphered key code, software with which said computer is provided, Memorize a collate program which cancels said code and compares a key code to memory storage, and said collate program memorized by said memory storage is executed at the time of use of said software, or installation, It has a means to compare whether a code of a key code stored in said recording medium and a key code memorized by storage parts store only for a key code of said computer is canceled, and these are in agreement, A protection system of computer software which makes improper use of a program in said computer, and installation when these key codes are not in agreement.

---

[Translation done.]

\* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

---

DETAILED DESCRIPTION

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the protection system and method of software especially about information processing systems, such as a computer which performs software.

[0002]

[Description of the Prior Art]In the computer, some following methods are used as a body surface thing from before as a method or a method for things other than a just user to prevent the software unauthorized use of the copy of software, installation, execution, etc.

[0003]The 1st method adds the dedicated hardware device for attestation to a main part.

[0004]The 2nd method performs use and non-use of the software in a computer based on the attestation judging by password input.

[0005]As the 3rd method, it leaves record of installation to the again recordable recording-medium side.

[0006]As what combined the above-mentioned method, for example to JP,9-34799,A. When the install program stored in CD-ROM is installed in the hard disk drive of a computer, An install program is made peculiar to a computer system by writing identification information, such as initialization time of a hard disk drive, in an install program, The identification information written in the install program when starting an install program and installing the data in CD-ROM on a hard disk, Only when the password from an input device is compared with the identification information which a computer system holds and these information consistents, the data protection method which permitted installation is proposed.

[0007]

[Problem(s) to be Solved by the Invention]However, the above-mentioned conventional protection method has a problem of the following statement.

[0008]In the case of the method which installs the hardware for attestation, have the problem that the cost of a product becomes high, and also. When using two or more software with which protection of the same kind is adopted, there is also a problem that the slots for the circuit of a computer body and a system configuration increasing, and connecting the hardware item for attestation, etc. run short etc.

[0009]In the conventional method which, on the other hand, performs use and non-use of software based on the attestation judging by password input, When an input becomes complicated when the length of a password is lengthened, and lengths of passwords are shortened, a password is detected easily and there is a problem that an attestation operation does not function effectively. Since the password information itself can be reproduced, functioning effectively as protection is not expectable.

[0010]And the conventional method of leaving record of installation to the again recordable recording-medium side has the problem that installation becomes again impossible, when internal storage breaks down.

[0011]Therefore, this invention is made in view of the above-mentioned problem, and the purpose, It is in providing the protection device and method of computer software by the unauthorized use of the software of the same medium by two or more computers, and the reproduced medium of preventing unjust use of software.

[0012]

[Means for Solving the Problem]This invention which attains said purpose enciphers a peculiar key code currently assigned for every computer, and carries out hold stores to a storage parts store only for a key code of said computer, A software provider demands a key code currently assigned in software to a computer which uses this software at the time of offer, A user who uses software by said computer, Supply a recording medium holding an encryption key code of a computer body, and a key code of an identical content to said software provider, and said software provider, After canceling encryption of a key code supplied from said computer and checking compatibility, A recording medium stored with said key code which enciphered software to provide, and a collate program which cancels said code and compares a key code is supplied to said computer, In said computer, said collate program stored in said recording medium is executed at the time of use of software recorded on said recording medium, or installation, Compare whether a code of a key code stored in said recording medium and a key code memorized by storage parts store only for a key code of said computer is canceled, and these are in agreement, and in not being in agreement, Unjust use of software by a medium by which software of the same medium by two or more computers was used improperly and reproduced by making improper use of a program in said computer and installation is prevented.

[0013]

[Embodiment of the Invention]An embodiment of the invention is described. Drawing 1 is a figure showing the composition of the 1 embodiment of this invention. In drawing 1, a peculiar key code (ID) is beforehand assigned to the computer 1, and it is, and preferably, it is enciphered and the hold stores of this key code are carried out to the storage parts store 2 only for a key code.

[0014]The donor of software demands the key code 21 currently assigned to the computer 1 which uses the software concerned by the device 4 for software offer at the time of offer of software.

[0015]The user who uses software on the computer 1 inputs the key code 21 of computer 1 main part, and the key code 31 of an identical content into the device 4 for software offer via the recording medium 3 only for a key code.

[0016]Thereby, with the device 4 for software offer, when recording the offer software to the program recording medium 5 of software, the inputted key code is recorded simultaneously.

[0017]A user at the time of use of the program recorded on the recording medium 5, or installation The key code 21 of computer 1 main part, In performing collation processing 6 with the key code 51 recorded on the medium 5 and not being in agreement as a result of collation, it makes impossible use of the program in the computer 1, and installation.

[0018]

[Example]The example of this invention is described in detail below with reference to drawings. Drawing 1 is a figure showing the composition of one example of this invention. Drawing 2 is a flow chart showing the procedure of one example of this invention.

As for (A), (B) shows [ software provider side ] users' procedure, respectively.

[0019]If drawing 1 and drawing 2 are referred to, the key code 21 peculiar at the time of manufacture, etc. is assigned by the computer 1.

It is preferably enciphered by the storage parts store 2 only for a key code inside a computer body, and it memorizes.

[0020]The hold stores of the program for canceling the code of the enciphered key code may be carried out to the storage parts store 2 only for this key code.

[0021]The storage parts store 2 only for this key code has been independent of other memory storage of the computer 1.

It is used only for \*\*\*\*\* and refer to the key code at the time of software using.

That is, reference of the direct information by the user (user) of the computer 1 and rewriting cannot be performed.

[0022]At the time of offer of software, the donor of software makes demands for the input of a key code on a user, and enciphers and records it on the recording medium 5 of software with

the software providing device 4.

[0023]In the software recording medium 5, the program 52 for performing the collation judgment of the enciphered key code 51 and the key code by the side of a recording medium and a computer body with the program 53 for offer (distribution) is recorded.

[0024]In the computer 1 at the user side at the time of the beginning of using of software, A collation judgment is performed, and when the key code 51 by the side of the software recording medium 5 and the key code 21 by the side of the computer body 1 are inharmonious, let use by computer 1 of the body program 53 stored in the software recording medium 5 be disapproval.

[0025]Operation of one example of this invention is explained.

[0026]A peculiar value is assigned for every computer at the time of manufacture of the computer 1, etc., and the key code 21 to the computer 1 is enciphered and memorized by the storage parts store 2 of an one computer inside-of-the-body part for exclusive use. The key code 21 consists of arbitrary text codes (alphanumeric character) putting together.

[0027]Although software is recorded on the external storage of the computer 1 and it is published (distribution), the device 4 of the side which provides software requires the input of a key code of the user of software at the time of the issue.

[0028]A key code is received and passed to the donor side of software via the external storage 3 for exclusive use with which the same key code as the one computer inside of the body was recorded beforehand. If it puts on delivery of this key code, it is expected that key code 21 the very thing will become complicated and huge, the alteration of that it is important not clarifying the contents of the key code 21 to the exterior and the key code 21 is not performed -- making -- in order to aim at things etc., it is made difficult to read or rewrite information generally, for example, media, such as a dedicated card with a built-in IC, are used. That is, in the computer 1, a user writes the key code 21 of the storage parts store 2 only for a key code in the recording medium 3 only for a key code, and equips the software provider device 4 of this recording medium 3.

[0029]The key code passed to the publisher side is once decoded with the software providing device 4 (Step A1 of drawing 2), Software offer is made disapproval when the compatibility is checked to see a key code is proper (Step A2 of drawing 2), and the key code does not consistent (step A5 of drawing 2).

[0030]When judged with the key code consistenting, it is again enciphered by the recording medium 5 and, simultaneously with record of the software (program 53) to provide, is recorded on it (step A4 of drawing 2).

[0031]As the recording medium 5 of the software at this time, also in order to avoid a next alteration etc., preferably, writing is made once into a limitation, and the recording medium which is not rewritable is used, for example, CD-ROM etc. are used.



[0032]The program 52 for performing the key code 51 and its collation processing other than the program body 53 of offer software is recorded on the recording medium 5.

[0033]The check of the key code by the side of computer 1 main part is performed based on the flow chart of drawing 2 (B). That is, the program 52 for keys matching is read from the software recording medium 5, and procedure of drawing 2 (B) is performed by executing this program. Namely, encryption of the key code 21 as which computer 1 main part was enciphered, and the key code 51 stored in the recording medium 5 is canceled, Both key codes are compared, and when in agreement, use of the body program 53 stored in the recording medium 5 is permitted, and when inharmonious, use of the body program 53 stored in the recording medium 5 is made improper.

[0034]In the case of the form of the program 53 which is a main part being temporarily read into the computer 1 from a medium, and operating, collation processing 6 of the key code by the side of a computer body and a recording medium is performed first, and when not in agreement, operation of the body program 53 is made improper.

[0035]When it is the form of operating after the body program 53 moves from on the external storage 5 on the internal storage of a computer and performs what is called installation, and a collated result is inharmonious, if it does so, \*\* of \*\*\*\*\* of installation will be made improper.

[0036]Next, the 2nd example of this invention is described. Drawing 3 is a figure showing the composition of the 2nd example of this invention. When drawing 3 is referred to, the connection between a software provider's device 40 and a user's computer body 1', It is carried out via the telephone line 20, and it is transmitted from the communication apparatus 11 and the information on the key code 21 that the main part of computer 1' was enciphered is directly transmitted to a software providing device 4' side through the telephone line 4.

[0037]In software providing device 4', as shown in drawing 2 (A), cancel the code of the key code transmitted from the computer 1' side, and the compatibility of a key code is checked, When the compatibility of a key code is checked, key code information is recorded on the inside of software providing device 4', and software and the information on a key code are directly replied to computer 1' through the telephone line 20.

[0038]The software (body program) replied via the telephone line 20 from software provider device 4', and the information on a key code, It is saved at the internal storage 3 of computer 1', and the key code returned from software provider device 4' and the key code 21 by the side of the computer body 1 are compared, and in being inharmonious, let use by computer 1 of a body program be disapproval.

[0039]When users' software is lost by causes, such as an obstacle, collation processing of a key code is performed by a software providing device 4' side about offer of the same software for the second time.

[0040]

[Effect of the Invention]As explained above, according to this invention, the effect of the following statement is done so.

[0041]The 1st effect of this invention is being able to prevent the software to provide from being unjustly used by two or more computers.

[0042]The recording medium which stored the software which provides the reason with a computer body in this invention supports 1 to 1.

It is because installation of the software in an inharmonious computer and execution are made into disapproval as a result of collation of the correspondence.

[0043]The 2nd effect of this invention is making it impossible to perform the unauthorized use by the duplicate of the recording medium itself.

[0044]In this invention, since information peculiar to a specific computer is held also at the reproduced recording medium, the reason is because it can be made to be able to operate on other computers.

---

[Translation done.]

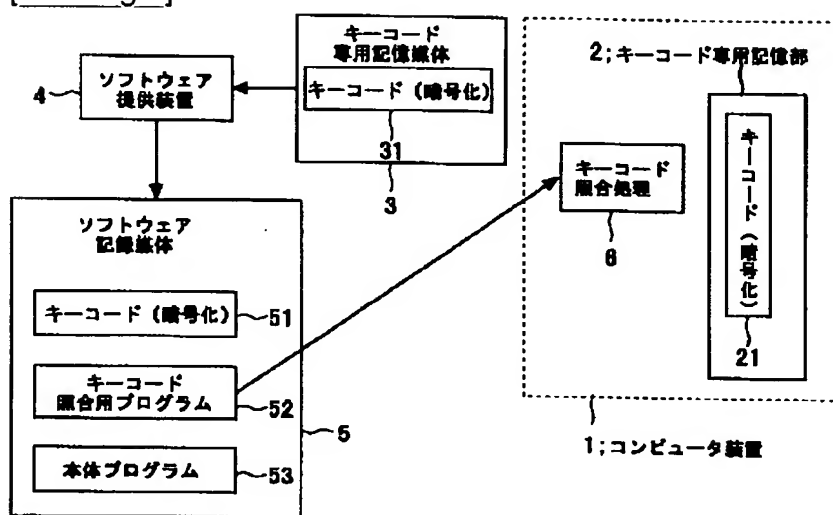
## \* NOTICES \*

JPO and INPIT are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.\*\*\*\* shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

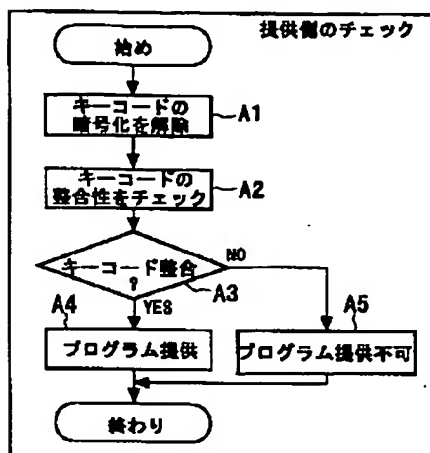
## DRAWINGS

[Drawing 1]

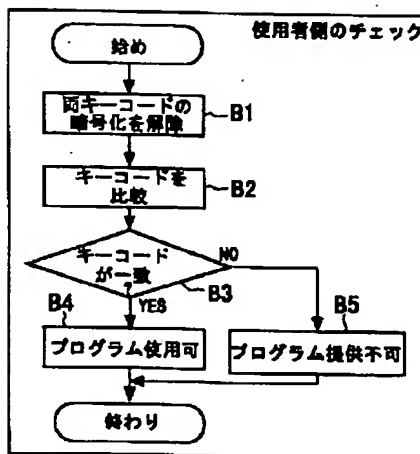


[Drawing 2]

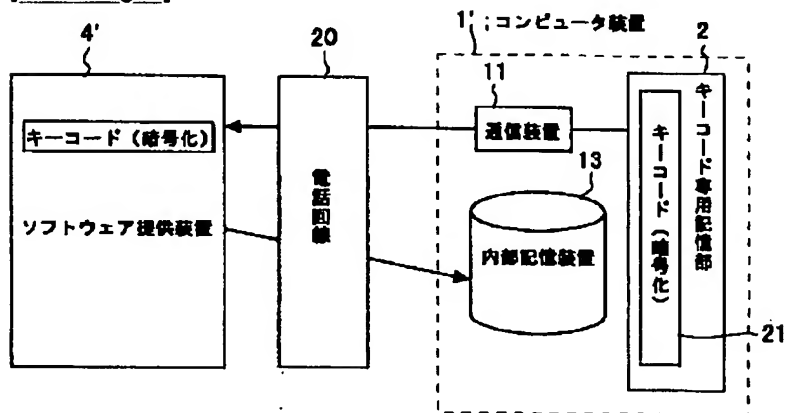
(A)



(B)



[Drawing 3]



[Translation done.]

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-207197

(43)Date of publication of application : 28.07.2000

(51)Int.Cl.

G06F 9/06

(21)Application number : 11-007269

(71)Applicant : NEC CORP

(22)Date of filing : 14.01.1999

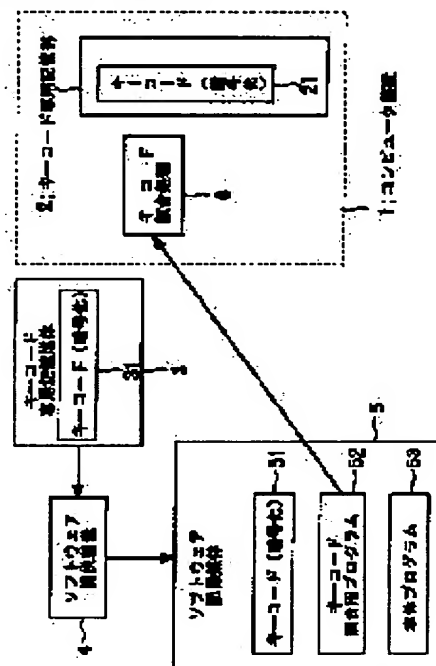
(72)Inventor : MURAMATSU KAZUE

## (54) SYSTEM AND METHOD FOR PROTECTING COMPUTER SOFTWARE

## (57)Abstract:

**PROBLEM TO BE SOLVED:** To prevent software from unauthorized use by collating identification information sent back from a software provider against the identification information of a computer.

**SOLUTION:** When providing a user with software, the software provider requests the user to input a key code and a software providing device 4 enciphers and records it on a recording medium of a software 5. On a software recording medium 5, the enciphered key code 51 and a program 52 for collating and deciding the key codes of the recording medium side and the computer main body side are recorded along with the provided (distributed) software 53. On the user's side, the computer 1 performs the collation and decision at the start of the use of the software and the use of the main body program 53 stored on the software recording medium 5 is made unauthorized, when the key code 51 on the side of the software recording medium 5 does not match the key code 21 of the computer main body 1.



(11)特許出願公開番号

特開2000-207197

(P2000-207197A)

(43)公開日 平成12年7月28日(2000.7.28)

(51) Int.Cl.<sup>7</sup>

G O 6 F 9/06

識別記号

550

FI

G O 6 F 9/06

テーマコード\* (参考)

550H 5B076

審査請求 有 請求項の数5 OL (全 7 頁)

(21)出願番号 特願平11-7269

(22)出願日 平成11年1月14日(1999.1.14)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 村松 一恵

東京都港区芝五丁目7番1号 日本電気株式会社内

(74) 代理人 100080816

弁理士 加藤 朝道

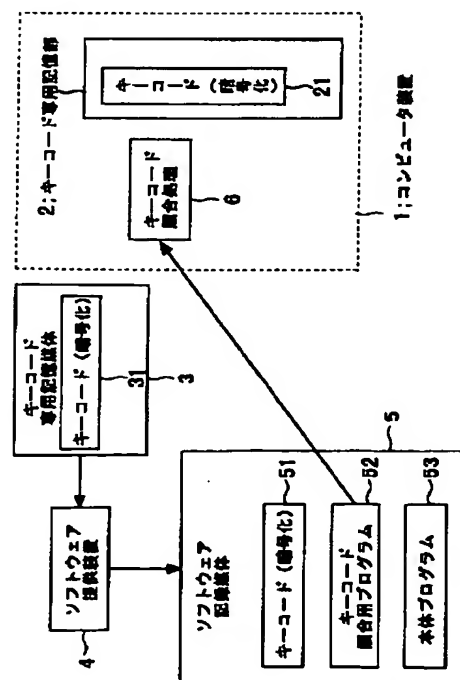
F.ターム(参考) 5B076 FB06 FB11

(54)【発明の名称】 コンピュータソフトウェアのプロテクトシステム及び方法

(57) 【要約】

【課題】複数のコンピュータによる同一媒体のソフトウェアの不正使用、複製された媒体による、ソフトウェアの不正な使用を防止するコンピュータソフトウェアのプロテクト方法の提供。

【解決手段】コンピュータ毎に割り当てられている固有のキーコードを暗号化してコンピュータに記憶保持し、ソフトウェア提供者側はソフトウェアを提供時に該ソフトウェアを使用するコンピュータのキーコードを要求し、ソフトウェア提供装置は、コンピュータのキーコードの暗号化を解除して整合性をチェックした後、提供するソフトウェアを、暗号化したキーコード、暗号を解除しキーコードを照合する照合プログラムとともに格納した記録媒体をコンピュータに供給し、コンピュータでは、記録媒体に記録されたソフトウェアの使用時、記録媒体のキーコードとコンピュータのキーコードの暗号を解除して照合し、一致しない場合には、コンピュータにおけるプログラムの使用、及びインストールを不可とする。



**【特許請求の範囲】**

【請求項1】ソフトウェア提供者からユーザにソフトウェアを提供するにあたり、前記ユーザから前記ユーザが使用するコンピュータが保有する固有の識別情報であって暗号化された識別情報を受け取り、ソフトウェア提供者側では、前記識別情報の暗号解読及び妥当性をチェックした上で、前記ユーザに配布するソフトウェアとともに、暗号化した状態の前記識別情報、及び、前記識別情報と前記ユーザのコンピュータの識別情報との照合処理を行なう照合判定プログラムを前記ユーザに提供し、前記ユーザが、前記ユーザのコンピュータで前記提供されたソフトウェアを使用する際、前記コンピュータ上で前記照合プログラムを実行して、ソフトウェア提供者から返送された識別情報と前記コンピュータの識別情報とが互いに一致するか否かを照合し、一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とする、コンピュータソフトウェアのプロテクト方法。

【請求項2】コンピュータ毎に割り当てられている固有のキーコードを暗号化して前記コンピュータのキーコード専用記憶部に記憶保持し、

ソフトウェア提供者は、ソフトウェアを提供時に該ソフトウェアを使用するコンピュータに割り当てられているキーコードを要求し、

前記コンピュータでソフトウェアを使用するユーザは、前記ソフトウェア提供者に、コンピュータ本体の暗号化キーコードと同一内容のキーコードを保持する記録媒体を供給し、

ソフトウェア提供者側装置は、前記コンピュータから供給されたキーコードの暗号化を解除して整合性をチェックした後、前記コンピュータに提供するソフトウェアを、暗号化した前記キーコード、前記暗号を解除しキーコードを照合する照合プログラムとともに格納した記録媒体を前記コンピュータに供給し、

前記コンピュータでは、ユーザが、前記記録媒体に記録されたソフトウェアの使用時、あるいはインストール時に、前記記録媒体に格納された前記照合プログラムを実行して、前記記録媒体に格納されたキーコードと、前記コンピュータの前記キーコード専用記憶部に記憶されているキーコードとの暗号を解除してこれらが一致するか否かを照合し、一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とする、コンピュータソフトウェアのプロテクト方法。

【請求項3】コンピュータ毎に割り当てられている固有のキーコードを暗号化して前記コンピュータのキーコード専用記憶部に記憶保持し、

ソフトウェア提供者は、ソフトウェアを提供時に該ソフトウェアを使用するコンピュータに割り当てられているキーコードを要求し、

前記コンピュータでソフトウェアを使用するユーザは、

前記ソフトウェア提供者に、コンピュータ本体の暗号化キーコードと同一内容のキーコードを通信回線を介して供給し、

前記ソフトウェア提供者側装置では、前記コンピュータから前記通信回線を介して供給されたキーコードの暗号化を解除して整合性をチェックした後、前記コンピュータに提供するソフトウェアを、暗号化した前記キーコード、暗号を解除しキーコードを照合する照合プログラムとともに前記通信回線を介して前記コンピュータに供給し、

前記コンピュータでは、前記通信回線を介して供給された、前記コンピュータに提供するソフトウェア、暗号化した前記キーコード、及び暗号を解除しキーコードを照合する照合プログラムと記憶装置に一旦記憶し、

前記ソフトウェアの使用時、あるいはインストール時に、前記記憶装置に格納された前記照合プログラムを実行して、前記記憶装置に格納されたキーコードと、前記コンピュータのキーコード専用記憶部に記憶されているキーコードの暗号を解除してこれらが一致するか否かを照合し、一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とする、コンピュータソフトウェアのプロテクト方法。

【請求項4】1又は複数のコンピュータと、該コンピュータにソフトウェアを提供するソフトウェア提供装置と、を備え、

前記各コンピュータは、コンピュータ毎に割り当てられている固有のキーコードを暗号化した状態で記憶保持するキーコード専用記憶部を備え、

ソフトウェア提供者は、ソフトウェアを提供時に、該ソフトウェアを使用するコンピュータに割り当てられているキーコードを要求し、

前記コンピュータでソフトウェアを使用するユーザは、前記ソフトウェア提供装置に、前記コンピュータ本体の暗号化キーコードと同一内容のキーコードを保持する記録媒体にて供給し、

前記ソフトウェア提供装置は、前記コンピュータから供給されたキーコードの暗号化を解除する手段と、

暗号が解除されたキーコードの整合性をチェックする手段と、

整合性のチェックされたキーコードを暗号化した状態で、前記コンピュータに提供するソフトウェア、及び、前記暗号を解除しキーコードを照合する照合プログラムとともに格納したソフトウェア記録媒体に書き込む手段と、

を備え、

前記ソフトウェア記録媒体を前記コンピュータに供給し、

前記ソフトウェア記録媒体を受け取った前記コンピュータが、前記ソフトウェア記録媒体に記録されたソフトウェアの使用時あるいはインストール時に、前記ソフトウ

ェ記録媒体に格納された前記照合プログラムを実行して、前記記録媒体に格納されたキーコードと、前記コンピュータのキーコード専用記憶部に記憶されているキーコードとの暗号を解除してこれらが一致するか否か照合する手段を備え、これらのキーコードが一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とする、コンピュータソフトウェアのプロテクトシステム。

【請求項5】1又は複数のコンピュータと、前記コンピュータに通信回線を介して接続され、前記コンピュータにソフトウェアを提供するソフトウェア提供装置と、を備え、

前記コンピュータは、コンピュータ毎に割り当てられている固有のキーコードを暗号化した状態で記憶保持するキーコード専用記憶部を備え、

ソフトウェア提供者は、ソフトウェアを提供時に、該ソフトウェアを使用するコンピュータに割り当てられているキーコードを要求し、

前記コンピュータでソフトウェアを使用するユーザは、前記ソフトウェア提供装置に、前記コンピュータ本体の暗号化キーコードと同一内容のキーコードを前記通信回線を介して前記ソフトウェア提供装置に送信し、

前記ソフトウェア提供装置は、前記コンピュータから前記通信回線を介して送信されたキーコードを受信してこのキーコードの暗号化を解除する手段と、

暗号が解除されたキーコードの整合性をチェックする手段と、

整合性のチェックされたキーコードを暗号化した状態で、前記コンピュータに提供するソフトウェア、及び、前記暗号を解除しキーコードを照合する照合プログラムとともに前記通信回線を介して前記コンピュータに送信する手段と、

を備え、

前記コンピュータが、前記ソフトウェア提供装置から前記通信回線を介して送信された、暗号化したキーコード、前記コンピュータに提供するソフトウェア、前記暗号を解除しキーコードを照合する照合プログラムを、記憶装置に記憶し、

前記ソフトウェアの使用時あるいはインストール時に、前記記憶装置に記憶された前記照合プログラムを実行して、前記記録媒体に格納されたキーコードと、前記コンピュータのキーコード専用記憶部に記憶されているキーコードの暗号を解除してこれらが一致するか否か照合する手段を備え、これらのキーコードが一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とする、コンピュータソフトウェアのプロテクトシステム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ソフトウェアを実

行するコンピュータ等の情報処理システムに関し、特に、ソフトウェアのプロテクトシステム及び方法に関する。

【0002】

【従来の技術】コンピュータにおいて、正当な使用者以外のものが、ソフトウェアの複製、インストール、実行等のソフトウェア不正使用を防止するための方法又は方式として、従来より、体系的なものとして、以下のようないくつかの方式が用いられている。

【0003】第1の方式は、認証用の専用ハードウェア装置を本体に追加する、というものである。

【0004】第2の方式は、コンピュータでのソフトウェアの使用・不使用を、パスワード入力による認証判定に基づき行う、というものである。

【0005】第3の方式として、再度記録可能な記録媒体側に、インストールの記録を残す、というものである。

【0006】さらに、上記方式を組み合わせたものとして、例えば特開平9-34799号公報には、CD-ROMに格納されたインストールプログラムをコンピュータのハードディスク装置にインストールする際、インストールプログラムにハードディスク装置の初期化日時等の識別情報を書き込むことでインストールプログラムをコンピュータシステム固有のものとし、インストールプログラムを起動してCD-ROM内のデータをハードディスクにインストールする際、インストールプログラムに書き込まれた識別情報と、コンピュータシステムが保有する識別情報と、入力装置からのパスワードを照合し、これらの情報が整合する場合にのみ、インストールを許可するようにしたデータプロテクト方法が提案されている。

【0007】

【発明が解決しようとする課題】しかしながら、上記した従来のプロテクト方式は下記記載の問題点を有している。

【0008】認証用ハードウェアを設置する方式の場合、製品のコストが高くなるという問題点を有しているほか、同種のプロテクトが採用されているソフトウェアを複数使用する場合に、コンピュータ本体の回路、システム構成が増大し、また認証用ハードウェア装置を接続するためのスロット等が不足する等といった問題点もある。

【0009】一方、ソフトウェアの使用・不使用を、パスワード入力による認証判定に基づき行う従来の方式において、パスワードの長さを長くした場合、入力が煩雑になり、またパスワード長を短くした場合には、パスワードが容易に見破られ、認証作用が有効に機能しない、という問題がある。さらに、パスワード情報そのものも複製可能であるため、プロテクトとして有効に機能することは期待できない。



【0010】そして、再度記録可能な記録媒体側に、インストールの記録を残すという従来の方法は、内部記憶装置が故障した場合等に、再度インストールが不可能となる、という問題点がある。

【0011】したがって、本発明は、上記問題点に鑑みてなされたものであって、その目的は、複数のコンピュータによる同一媒体のソフトウェアの不正使用、複製された媒体による、ソフトウェアの不正な使用を防止するコンピュータソフトウェアのプロテクト装置及び方法を提供することにある。

【0012】

【課題を解決するための手段】前記目的を達成する本発明は、コンピュータ毎に割り当てられている固有のキーコードを暗号化して前記コンピュータのキーコード専用記憶部に記憶保持し、ソフトウェア提供者は、ソフトウェアを提供時に該ソフトウェアを使用するコンピュータに割り当てられているキーコードを要求し、前記コンピュータでソフトウェアを使用するユーザは、前記ソフトウェア提供者に、コンピュータ本体の暗号化キーコードと同一内容のキーコードを保持する記録媒体を供給し、前記ソフトウェア提供者は、前記コンピュータから供給されたキーコードの暗号化を解除して整合性をチェックした後、提供するソフトウェアを、暗号化した前記キーコード、前記暗号を解除しキーコードを照合する照合プログラムとともに格納した記録媒体を前記コンピュータに供給し、前記コンピュータでは、前記記録媒体に記録されたソフトウェアの使用時、あるいはインストール時に、前記記録媒体に格納された前記照合プログラムを実行して、前記記録媒体に格納されたキーコードと、前記コンピュータのキーコード専用記憶部に記憶されているキーコードの暗号を解除してこれらが一致するか否かを照合し、一致しない場合には、前記コンピュータにおけるプログラムの使用、及びインストールを不可とすることで、複数のコンピュータによる同一媒体のソフトウェアの不正使用、ならびに複製された媒体による、ソフトウェアの不正な使用を防止するものである。

【0013】

【発明の実施の形態】本発明の実施の形態について説明する。図1は、本発明の一実施の形態の構成を示す図である。図1において、コンピュータ1には、固有のキーコード(1D)が予め割り当てられおり、該キーコードは、好ましくは暗号化されてキーコード専用記憶部2に記憶保持されている。

【0014】ソフトウェアの提供者は、ソフトウェアの提供時に、ソフトウェア提供用装置4によって、当該ソフトウェアを使用するコンピュータ1に割り当てられているキーコード21を要求する。

【0015】コンピュータ1上でソフトウェアを使用するユーザは、キーコード専用記録媒体3を介して、ソフトウェア提供用装置4に、コンピュータ1本体のキーコ

ード21と同一内容のキーコード31を入力する。

【0016】これにより、ソフトウェア提供用装置4で、ソフトウェアのプログラム記録媒体5への提供ソフトウェアを記録する時に、入力されたキーコードが同時に記録される。

【0017】ユーザが、記録媒体5に記録されたプログラムの使用時、あるいはインストール時に、コンピュータ1本体のキーコード21と、媒体5に記録されたキーコード51との照合処理6を行い、照合の結果、一致しない場合には、コンピュータ1におけるプログラムの使用、及びインストールを不可能とする。

【0018】

【実施例】本発明の実施例について図面を参照して以下に詳細に説明する。図1は、本発明の一実施例の構成を示す図である。図2は、本発明の一実施例の処理手順を示す流れ図であり、(A)はソフトウェア提供者側、(B)はユーザ側の処理手順をそれぞれ示している。

【0019】図1及び図2を参照すると、コンピュータ1には、製造時等に固有のキーコード21が割り振られており、コンピュータ本体内部のキーコード専用記憶部2に、好ましくは暗号化されて記憶されている。

【0020】このキーコード専用記憶部2には、暗号化されたキーコードの暗号を解除するためのプログラムを記憶保持してもよい。

【0021】このキーコード専用記憶部2は、コンピュータ1の他の記憶装置からは独立しており、キーコードの保存及びソフトウェア使用時のキーコード参照のためにだけに利用される。すなわちコンピュータ1のユーザ(使用者)による直接の情報の参照、及び書換えは行えない。

【0022】ソフトウェアの提供者は、ソフトウェアの提供時に、使用者に対してキーコードの入力を要求し、ソフトウェア提供装置4により、ソフトウェアの記録媒体5に暗号化して記録する。

【0023】ソフトウェア記録媒体5内には、提供(配布)対象のプログラム53とともに、暗号化されたキーコード51と、記録媒体側とコンピュータ本体側とのキーコードの照合判定を行うためのプログラム52とが記録されている。

【0024】使用者側では、ソフトウェアの使用開始時に、コンピュータ1において、照合判定を行い、ソフトウェア記録媒体5側のキーコード51とコンピュータ本体1側のキーコード21が不一致の場合には、ソフトウェア記録媒体5に格納された本体プログラム53のコンピュータ1での使用を不許可とする。

【0025】本発明の一実施例の動作について説明する。

【0026】コンピュータ1に対するキーコード21は、コンピュータ1の製造時等にコンピュータ毎に固有の値が割り振られ、コンピュータ1本体内部の専用の記

憶部2に暗号化して記憶される。キーコード21は、任意のテキストコード（英数字）の組合せ）からなる。

【0027】ソフトウェアは、コンピュータ1の外部記憶媒体に記録されて発行（配布）されるが、その発行時に、ソフトウェアを提供する側の装置4がソフトウェアの利用者に対しキーコードの入力を要求する。

【0028】キーコードは、あらかじめコンピュータ1本体内と同一のキーコードが記録された専用の外部記憶媒体3を介して、ソフトウェアの提供者側に受け渡される。このキーコードの受け渡しに置いては、キーコード21自体が複雑且つ長大なものとなる事が予想されること、キーコード21の内容を外部に對し明らかにしない事が肝要であること、キーコード21の改竄が行われないようにすること、等を目的とするため、一般的に情報を読み出したり書き換えたりすることが困難とされている、例えばIC内蔵の専用カード等の媒体が用いられる。すなわち、コンピュータ1において使用者は、キーコード専用記憶部2のキーコード21をキーコード専用記録媒体3に書き込み、この記録媒体3のソフトウェア提供者装置4に装着する。

【0029】発行者側に渡されたキーコードは、ソフトウェア提供装置4で一旦解読され（図2のステップA1）、キーコードが適正なものであるかその整合性がチェックされ（図2のステップA2）、キーコードが整合していない場合、ソフトウェア提供を不許可とする（図2のステップA5）。

【0030】キーコードが整合していると判定された場合、提供するソフトウェア（プログラム53）の記録と同時に、記録媒体5に再度暗号化されて記録される（図2のステップA4）。

【0031】この時のソフトウェアの記録媒体5としては、後の改竄等を回避するためにも、好ましくは、書き込みが一回限りとされ、書き換えが不可能な記録媒体が用いられ、例えばCD-ROM等が用いられる。

【0032】記録媒体5には、提供ソフトウェアのプログラム本体53の他に、キーコード51及び、その照合処理を行うためのプログラム52が記録されている。

【0033】コンピュータ1本体側でのキーコードのチェックは、図2（B）の流れ図に基づいて行われる。すなわち、ソフトウェア記録媒体5からキー照合用プログラム52を読み込み、このプログラムを実行することで、図2（B）の処理手順が実行される。すなわち、コンピュータ1本体の暗号化されたキーコード21、記録媒体5に格納されたキーコード51の暗号化を解除し、両キーコードを比較し、一致している場合、記録媒体5に格納されている本体プログラム53の使用を許可し、不一致の場合、記録媒体5に格納されている本体プログラム53の使用を不可とする。

【0034】本体であるプログラム53が媒体から一時的にコンピュータ1に読み込まれて動作する形式の場

合、最初にコンピュータ本体側と記録媒体側でのキーコードの照合処理6が行われ、一致しない場合本体プログラム53の動作を不可とする。

【0035】また、本体プログラム53が、外部記憶媒体5上からコンピュータの内部記憶装置上に移し替え、いわゆるインストールを行ってから動作する形式である場合、照合結果が不一致である場合、そうしたらインストールの動作そのものを不可とする。

【0036】次に、本発明の第2の実施例について説明する。図3は、本発明の第2の実施例の構成を示す図である。図3を参照すると、ソフトウェア提供者の装置40と利用者のコンピュータ本体1'との接続は、電話回線20を介して行われ、コンピュータ1'の本体の暗号化されたキーコード21の情報は、通信装置11から送信され、電話回線4を通じてソフトウェア提供装置4'側に直接送信される。

【0037】ソフトウェア提供装置4'では、図2（A）に示したように、コンピュータ1'側から送信されたキーコードの暗号を解除してキーコードの整合性をチェックし、キーコードの整合性が確認された場合、キーコード情報をソフトウェア提供装置4'の内部に記録し、電話回線20を通じて、直接、ソフトウェア及びキーコードの情報をコンピュータ1'に返信する。

【0038】ソフトウェア提供者装置4'から電話回線20を介して返信されたソフトウェア（本体プログラム）及びキーコードの情報は、コンピュータ1'の内部記憶装置3に保存され、ソフトウェア提供者装置4'から返送されたキーコードとコンピュータ本体1側のキーコード21とを照合し、不一致の場合には、本体プログラムのコンピュータ1での使用を不許可とする。

【0039】また障害等の原因で、使用者側のソフトウェアが失われた場合、同一ソフトウェアの再度の提供に関して、ソフトウェア提供装置4'側でキーコードの照合処理が行われる。

【0040】

【発明の効果】以上説明したように、本発明によれば下記記載の効果を奏する。

【0041】本発明の第1の効果は、提供するソフトウェアが複数のコンピュータで不正に使用されることを防止することができる、ということである。

【0042】その理由は、本発明においては、コンピュータ本体と、提供するソフトウェアを格納した記録媒体とが1対1に対応しており、その対応の照合の結果、不一致のコンピュータでのソフトウェアのインストール、実行を不許可としている、ためである。

【0043】本発明の第2の効果は、記録媒体自体の複製による不正使用を行うことを不可能としている、ということである。

【0044】その理由は、本発明においては、複製された記録媒体にも、特定のコンピュータ固有の情報が保持

されるため、他のコンピュータ上では動作させる、ことができないためである。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示す図である。

【図2】本発明の一実施例の処理手順を示す流れ図であり、(A)はソフトウェア提供者側、(B)はユーザ側の処理手順の流れ図である。

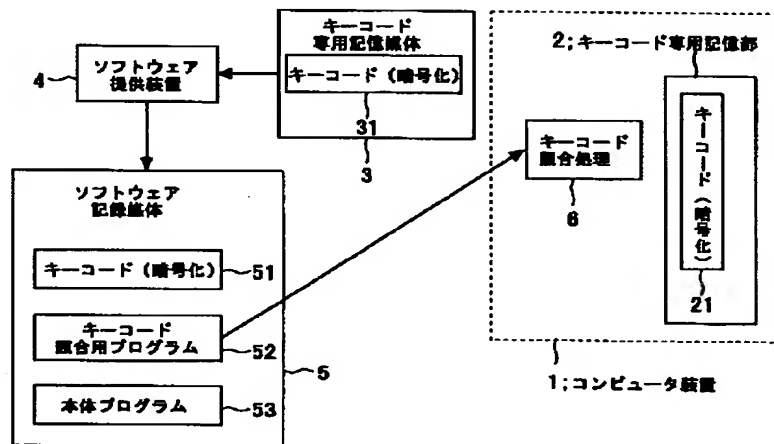
【図3】本発明の第2の実施例の構成を示す図である。

【符号の説明】

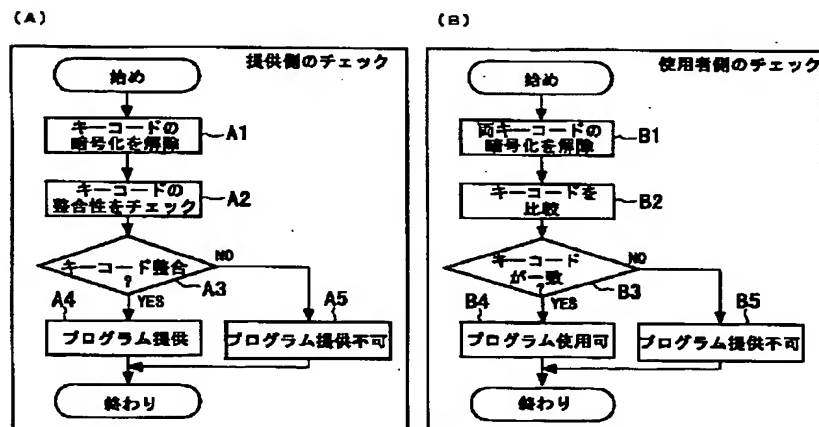
- 1 コンピュータ  
2 キーコード専用記憶部

- 3 キーコード専用記憶媒体  
4 ソフトウェア提供装置  
5 ソフトウェア記録媒体  
11 通信装置  
13 内部記憶装置  
20 電話回線  
21 キーコード  
31 キーコード  
51 キーコード  
52 キーコード照合用プログラム  
53 本体プログラム

【図1】



【図2】



【図3】

